[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 9/06

[12]发明专利申请公开说明书

[21]申请号 00800611.3

[43]公开日 2001年7月4日

[11]公开号 CN 1302399A

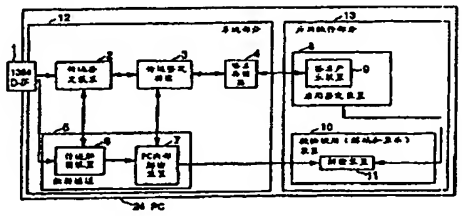
[22]申请日 2000.2.21 [21]申请号 00800611.3
[30]优先权
[32]1999.2.22 [33]JP [31]043870/1999
[86]国际申请 PCT/JP00/00956 2000.2.21
[87]国际公布 WO00/50989 日 2000.8.31
[85]进入国家阶段日期 2000.12.18
[71]申请人 松下电器产业株式会社
地址 日本国大阪府门真市
[72]发明人 武知秀明 山田正纯 饭冢裕之
西村拓也 久野良树 后藤昌一
[74]专利代理机构 上海专利商标事务所
代理人 孙敬国

权利要求书2页 说明书18页 附图页数7页

[54]发明名称 计算机和程序记录媒体

[57]摘要

要解决的问题是:一旦版权保护的AV数据传送到应用软件,该应用软件 就能随便处理该AV数据等,从而失去版权保护的目的。本发明提供一种计算 机,它包含系统部分12和应用软件部分13,在版权保护中,该计算机经数字接 口1取加密数据,进行处理,其中,所述系统部分12对所述应用软件部分13是 对版权保护合法的应用软件进行判断,如果所述应用软件是合法的应用软件,系 统部分12传送所述加密数据的密钥到应用软件部分13。



ISSN1008-4274

权 利 要 求 书

1. 一种计算机，包含系统部分和应用软件部分，在版权保护中，该计算机经数字接口取加密数据，进行处理，其特征在于，其中

所述系统部分对所述应用软件部分是对版权保护合法的应用软件进行判断，并且

如果所述应用软件是合法的应用软件，所述系统部分传送所述加密数据的密钥到所述应用软件部分。

2. 根据权利要求 1 所述的计算机，其特征在于，其中，所述系统部分中的判断是通过在所述系统部分与所述应用软件部分之间进行鉴定进行的。

3. 根据权利要求 1 所述的计算机，其特征在于，其中，所述系统部分中的判断是通过使用列有非法或合法应用软件的证件注销表进行的。

4. 根据权利要求 1 到 3 任一权利要求所述的计算机，其特征在于，其中，所述系统部分作为与外部装置鉴定的结果获得所述加密的密钥，对所述加密的数据进行解密，并用所述密钥或另一密钥对所述解密的数据再一次加密。

5. 根据权利要求 1 到 4 任一权利要求所述的计算机，其特征在于，其中，所述系统部分包含篡改验证功能，篡改码插在所述应用软件部分中的所述应用软件中，所述系统部分从所述应用软件部分读出所述篡改码，并使用所述篡改验证功能验证所述应用软件是否被篡改，若发现所述应用软件已篡改，则所述系统部分报告所述验证结果。

6. 一种计算机，包含系统部分和应用软件部分，在版权保护中，该计算机经数字接口取加密数据，进行处理，其特征在于，其中

所述系统部分包含多种篡改验证功能；与指定类型的篡改验证功能关联的篡改码和表明所述类型的类型信息嵌入所述应用软件部分中的所述应用软件中；其中，所述系统部分从所述应用软件部分读出所述篡改码和它的相关类型信息，并使用对应所述类型的篡改验证功能验证所述应用软件是否被篡改，若发现所述应用软件已篡改，则所述系统部分报告所述验证结果。

7. 一种计算机，包含系统部分和应用软件部分，在版权保护中，该计算机经数字接口取加密数据，进行处理，其特征在于，其中

所述系统部分通过嵌入与驻留在所述应用软件部分中的应用软件相关的所述数据信息，发送所述数据到所述应用软件部分。

8. 根据权利要求 7 所述的计算机，其特征在于，其中，与所述应用软件有关的信息是表明所述应用软件的名称、所述应用软件的版本号、篡改码或防篡改验证功能的类型的信息，或涉及用户的信息。

9. 一种媒体，其特征在于，该媒体存有程序和/或数据，使计算机能执行权利要求 1 至权利要求 8 任一权利要求中所描述的部分或全部装置的部分或全部功能，其中，所述媒体是计算机可处理的媒体.

10. 一种信息集，其特征在于，其中，所述信息集是程序和/或数据，使计算机能执行 1 至 8 任一权利要求中所描述的部分或全部装置的部分或全部功能。

说　明　书

计算机和程序记录媒体

技术领域

本发明涉及用于记录和再现数据的计算机，还涉及程序记录媒体。

背景技术

以数字形式传送音频和视频信息的网络正在发展。为了传送可视听的音频、视频信息，数据必须实时发送。

IEEE 1394 被建议用作网络实现实时传送的标准，现今已得到广泛地使用。IEEE 1394 作为外部接口安装在许多数字视频/音频设备上，包括家用数字 VCR。在 VCR 中，IEEE 1394 的应用已经能从外部装置控制 VCR，也能从外部装置将数据发送给 VCR，用于记录和再现。

此外，在 PC 中，随着多媒体技术的开发和像大容量硬盘和磁光盘记录媒体的到来，变得也能处理音频和视频信息。也即，目前 PC 能够具有对音频和视频信息记录和再现的装置的功能。例如，视窗 98，PC 的标准 OS(操作系统)，支持 IEEE 1394，使得它能在 PC 与数字音频/视频装置，如 VCR 之间传送 AV 数据。因此，可预见到 PC 和数字视频/音频装置的熔合在未来会得到进步的发展。

为了能够处理视频和音频信息，必须将处理视频和音频的应用软件安装到 PC(个人计算机)上。借助安装在 PC 的应用软件将视频/音频装置传送来的 AV 数据输入 PC 并经处理，用于显示、记录、再现等。例如，若应用软件是一种具有记录功能的软件，则通过该软件将视频/音频装置传送来的 AV 数据输入到 PC 并记录在如硬盘或磁光盘的记录媒体上。因而，能够处理 AV 数据的应用软件提供各种性能，通过安装这样的应用软件，PC 能增加如记录、再现、显示和处理控制等 AV 数据处理的各种功能。

某些 AV 数据通过例如禁止拷贝或只让拷贝一次来要求版权保护。在像这样的 VCR 数字视频/音频装置中，通过遵守主张的版权保护状态可记录或重放这种获得版权的 AV 数据。例如，VCR 不记录禁止拷贝的 AV 数据。相反，VCR 允许记录只让拷贝一次的 AV 数据。通过在 VCR 和 AV 数据发送装置，如 STB(卫星广播接收机)之间交换基于版权的鉴定或使用许可信息，证实是否允许拷贝 AV 数据。

然而，当今的 PC，由于 PC 可通过使用安装其上的应用软件的功能而具有例如记录、再现和显示等各种功能，因而即使某人想遵守授有版权的 AV 数据的版权，也会出现这样的问题，即，一旦授有版权的 AV 数据经过所述应用软件，人们通过使用应用软件能自由地处理该 AV 数据，用于记录等，从而失去版权保护的目的。

即便设计一种机构对应用软件附加许可处理授版权的 AV 数据，如果应用软件被非法修改，则版权不可能被保护。在这种情况下，如果在应用软件中设有防篡改系统防止非法修改应用软件，则版权能得到有效的保护。但是，该方法不是没有问题，也即，一旦该防篡改系统被非法用户攻破，则不但对 PC 机构，而且对 OS 结构，应用软件等都会发生实质性的变化，从而导致大量损失。

而且，如果使用未授与如上所述许可的应用软件非法处理授版权的数据，则根据被应用软件非法拷贝和分发的数据不能够识别该源应用软件。也即，即使知道存在非法应用软件，则也不能够检测和阻止使用非法应用软件。也就是说，问题在于不可能为版权保护目的来识别和消除非法软件。

利用软件非法使用的一个特征是，这种非法使用的方法只要拷贝到软件就能广泛地传播。这样产生的问题是，即便能识别非法传播的源，在硬件阻止非法装置使用的情况下，也不可能有效地逐个装置采用一种方法加以阻止。例如，当能够逃避防篡改系统检查的非法改变的应用软件的拷贝传播时，或发现逃避防篡改系统检查的方法并得到传播时，用先前已知的阻止各个计算机使用的方法不能够防止这种非法行为；此外，还会防碍软件的正常应用。

鉴于上述情况，很明显，一旦发现为非法传播目的而修改计算机进行非法流传时，由于不得不在计算机上或 OS 上禁止使用 AV 数据和修改计算机或 OS 本身，因此，损害是广泛的，所涉及的费用非常高。

如上所述，问题在于一旦授版权的数据非法流传，不能找到有效的方法阻止非法使用。

本发明揭示

存在的问题是：应用软件能实现对授予版权的数据侵权的处理，攻破版权保护目的；通过非法修改应用软件可攻破版权保护是实际存在的；如果产生非法应用软件，则不可能识别和阻止非法软件的侵权；如果能够逃避防篡改系统检查的非法改变的应用软件的拷贝得到流传，则用已知的方法不可能防止非法使用；和当发现为非法流传目的而修改的计算机非法流传时，采取对策的费用非常高。鉴

于上述问题，本发明的目的在于提供一种计算机和程序记录媒体，它能对授版权的数据进行版权保护并针对非法修改应用软件采取对策，而且，如果发现非法应用软件，则能识别和拒绝该应用软件并能防止非法流传而不涉及额外费用。

为了解决上面描述的问题，本发明的第 1 发明(对应权利要求 1)是

一种计算机，包含系统部分和应用软件部分，在版权保护中，该计算机经数字接口取加密数据，进行处理，其中

所述系统部分对所述应用软件部分是对版权保护合法的应用软件进行判断，并且

如果所述应用软件是合法的应用软件，所述系统部分传送所述加密数据的密钥到所述应用软件部分。

本发明第 2 发明(对应权利要求 2)是根据所述第 1 发明的计算机，其中，所述系统部分中的判断是通过在所述系统部分与所述应用软件部分之间进行鉴定进行的。

本发明第 3 发明(对应权利要求 3)是根据所述第 1 发明的计算机，其中，所述系统部分中的判断是通过使用列有非法或合法应用软件的证件注销表进行的。

本发明第 4 发明(对应权利要求 4)是根据所述第 1 到第 3 发明的任一发明的计算机，其中，所述系统部分作为与外部装置鉴定的结果获得所述加密的密钥，对所述加密的数据进行解密，并用所述密钥或另一密钥对所述解密的数据再一次加密。

本发明第 5 发明(对应权利要求 5)是根据所述第 1 到第 4 发明的任一发明的计算机，其中，所述系统部分包含篡改验证功能，篡改码插在所述应用软件部分中的所述应用软件中，所述系统部分从所述应用软件部分读出所述篡改码，并使用所述篡改验证功能验证所述应用软件是否被篡改，若发现所述应用软件已篡改，则所述系统部分报告所述验证结果。

本发明的第 6 发明(对应权利要求 6)是一种计算机，包含系统部分和应用软件部分，在版权保护中，该计算机经数字接口取加密数据，进行处理，其中

所述系统部分包含多种篡改验证功能；与指定类型的篡改验证功能关联的篡改码和表明所述类型的类型信息嵌入所述应用软件部分中的所述应用软件中；其中，所述系统部分从所述应用软件部分读出所述篡改码和它的相关类型信息，并使用对应所述类型的篡改验证功能验证所述应用软件是否被篡改，若发现所述应用软件已篡改，则所述系统部分报告所述验证结果。

本发明的第 7 发明(对应权利要求 7)是一种计算机，包含系统部分和应用软件部分，在版权保护中，该计算机经数字接口取加密数据，进行处理，其中

所述系统部分通过嵌入与驻留在所述应用软件部分中的应用软件相关的所述数据信息，发送所述数据到所述应用软件部分。

本发明第 8 发明(对应权利要求 8)是根据所述第 7 发明的计算机，其中，与所述应用软件有关的信息是表明所述应用软件的名称、所述应用软件的版本号、篡改码、或防篡改验证功能的类型的信息，或涉及用户的信息。

本发明第 9 发明(对应权利要求 9)是一种媒体，该媒体存有程序和/或数据，使计算机能执行第 1 至第 8 发明任一发明中所描述的部分或全部装置的部分或全部功能，其中，所述媒体是计算机可处理的媒体.

本发明第 10 发明(对应权利要求 10)是一种信息集，其中，所述信息集是程序和/或数据，使计算机能执行第 1 至第 8 发明任一发明中所描述的部分或全部装置的部分或全部功能。

附图概述

图 1 为示出本发明第 1 实施例的方框图，其中，鉴定是在系统部分和应用软件部分之间进行的，AV 数据在 PC 中加密。

图 2 为示出本发明第 2 实施例的方框图，其中，使用 CRL 检测非法应用软件。

图 3 为示出本发明第 3 实施例的方框图，其中，结合有防篡改系统。

图 4 为示出本发明第 4 实施例的方框图，其中，结合有多种篡验证功能。

图 5 为示出本发明第 5 实施例的方框图，其中，电子水印嵌入到受版权保护的 AV 数据中。

图 6 为示出本发明第 6 实施例的方框图，其中，受版权保护的 AV 数据的版权能保护得更安全。

图 7 为示出按照本发明第 1 实施例的鉴定成功/失败状态相对附加于应用软件的许可类型的表。

[参考号的说明]

1. 1394 D－IF

2. 传送鉴定装置

3. 应用鉴定功能

4. 签名存储器

5. 数据通道

6. 传送解密装置

7. PC 内的加密装置

8. 应用鉴定装置

9. 签名产生装置

10. 数据使用(解码显示)装置

11. 解密装置

12. 系统部分

13. 应用软件部分

14. CRL 存储器

15. 应用 CRL 存储器

16. CRL 比较装置

17. 篡改鉴定功能

18. 19. 软件检查装置

20. 版本选择装置

21. 篡改鉴定功能

22. 签名嵌入装置

23. 电子水印嵌入装置

实施本发明的最佳形态

下面参照附图描述本发明的实施例。

(实施例 1)

参照图 1 和图 7 描述第 1 实施例。该实施例处理的情况是，鉴定在系统部分与应用软件部分之间进行，且输入到 PC 的 AV 数据经 PC 以加密形式传送。在图 1 中，PC24 包含系统 12 和应用软件部分 13。系统部分 12 是 PC24 的 D—IF 硬件或像驱动器或 OS 的系统软件。应用软件部分 13 是记录应用软件和执行该应用软件的装置。

系统部分 12 包含 1394 D—IF 1，传送鉴定装置 2，应用鉴定功能 3，签名存储器 4，传送解密装置 6 和 PC 内部加密装置 7。

1394 D—IF 1 是 IEEE 1394 接口，一种串行总线接口标准，用于传送到和来自像 STB 或 D—VHS 的外部装置的数据和指令。传送鉴定装置 2 是这样一种装置，

即当 AV 数据要求版权保护时，与外部装置执行鉴定，当鉴定成功完成时，传送对 AV 数据解密的密钥到传送解密装置 6。应用鉴定功能是一种当经过 1394 D－IF 1 输入的 AV 数据请求版权保护时在 PC 内进行鉴定的手段。具体而言，通过参照签名存储器 4 中的内容，用应用软件部分 13 进行鉴定，由签名产生装置 9 产生的签名记录在签名存储装置 4 中，当鉴定成功完成时，将加密密钥传送到 PC 内的加密装置 7 并将解密密钥传送到应用鉴定装置 8。签名存储器 4 是一种记录签名产生装置 9 产生签名的存储器。传送解密装置 6 是一种当与外部装置成功完成鉴定时从传送鉴定装置 2 接收密钥并对经 1394 D－IF 1 输入的 AV 数据进行解密的装置。PC 内部的加密装置 7 是一种当与应用软件部分 13 成功完成鉴定时对传送解密装置 6 解密的 AV 数据重新加密并将该加密后的数据传送到应用软件部分 13 的装置。

应用软件部分 13 包含应用鉴定装置 8，签名产生装置 9，数据使用(解码和显示)装置 10，和解密装置 11。

应用鉴定装置 8 是一种用系统部分 12 中应用鉴定功能进行鉴定的装置。签名产生装置 9 是一种产生数字签名的装置，当用系统部分 12 进行鉴定时使用该数字签名。数据使用(解码和显示)装置 10 是一种使当前运行的应用软件能使用 AV 数据的装置。解密装置 11 是一种当用系统部分 12 成功完成鉴定时从应用鉴定装置 9 接收解密密钥并使用该密钥对 PC 内部加密装置 7 加密的 AV 数据进行解密的装置。

接下来，描述具有上述构成的该实施例的运作。首先说明描述版权信息的方法。

当 AV 数据从如 STB 或 VTR 等外部装置传送到 PC 24 时，该 AV 数据可能是要求版权保护的数据。也即，它可能带有附加部分表明禁止拷贝或只允许拷贝一次。这种表明使用认可的信令信息用嵌入数据流中的 CGMS(拷贝代信息)实现。

CGMS 包含在从广播站发来的传输流中。CGMS 是 2 比特数据；该 CGMS 能取的值和这些值的含义如下。

也即，CGMS＝11 表示“不允许拷贝”，CGMS＝10 表示“拷贝一代”，CGMS＝00 表示“任意拷贝”。CGMS＝01 不存在。这里，“不允许拷贝”表示禁止拷贝并只允许播放 AV 数据。“拷贝一代”表示拷贝只允许一次且拷贝的 AV 数据如上所述可播放许多次。“任意拷贝”表示数据可随便拷贝。检测 CGMS 需要提供传输流解码器电路等，从而使硬件结构复杂化。

如果在 IEEE 1394 包数据标题中包含传送使用允许信息的信令信息(下文称

为加密方式指示器EMI)，则可不用像传输流解码器电路那样的硬件。

EMI产生于CGMS，并取下面的值，即，EMI＝11表示“不允许拷贝”，EMI＝10表示“拷贝一代”，EMI＝00表示“任意拷贝”。EMI＝01“不再拷贝”。这里，“不允许拷贝”表示禁止拷贝并且只允许播放AV数据。“拷贝一代”表示拷贝只允许一次且拷贝的AV数据如上所述可播放许多次。“任意拷贝”表示数据可随便拷贝。“不再拷贝”表示数据是按照“拷贝一代”已经拷贝过的AV数据，因此，不允许再拷贝。

在IEEE 1394中，这种EMI用来指定加密的方法和鉴定的方法。例如，当用表示“任意拷贝”的EMI发送AV数据时，不进行加密。对于带有表示“拷贝一代”的EMI＝10，或表示“不再拷贝”的EMI＝01的数据，其用于加密的密钥和装置鉴定的方法与带有表示“不允许拷贝”的EMI＝11的数据所用的不同。

这里，假定AV数据是从STB接收到的。接着，根据CGMS或EMI确定从STB接收到的AV数据是否为要求版权保护的数据；如果是要求版权保护的数据，则用STB(AV数据的发送者)进行鉴定。AV数据以加密形式发送，当成功完成鉴定时，传送鉴定装置2从STB接收对AV数据解密的密钥。当EMI为11时，鉴定将根据公共密钥(public key)进行，而当EMI为10或01时，鉴定将根据普通密钥(common key)进行。

当在传送鉴定装置与STB之间成功地完成鉴定时，接着在应用软件部分13与系统部分12之间进行鉴定。在应用鉴定装置8，签名产生装置9对当前运行的应用软件产生数字签名。签名存储器4记录签名产生装置8产生的数字签名。应用鉴定功能3通过使用记录在签名存储器4中的数字签名，用应用鉴定装置8进行鉴定。

对应要求版权AV数据的使用允许信息的许可预先附加到各应用软件。只要软件有合法的许可，则应用软件部分13与系统部分12间的鉴定就能成功地完成。具体而言，许可按照应用软件的功能分类。也就说，对于只有显示AV数据功能的软件所给的许可被分类为许可A，对于具有记录AV数据功能的软件所给的许可被分类为许可B。对于严格遵守拷贝保护状态的软件所给的许可被分类为许可C。赋予这样软件许可C，使得当AV数据是禁止拷贝数据时，只能播放该AV数据而不能拷贝它，当AV数据是允许只拷贝一次的数据时，只能拷贝一次。但是，该许可C要求连同AV数据向应用软件报告版权保护数据的版权内容；这通过向AV数据建立EMI或CGMS来完成。

这里，假定当前运行的应用软件的许可类别是 B。也假定从 STB 发送的 AV 数据的使用允许信息表明 EMI＝11。也即，禁止拷贝 AV 数据。在这种情况下，在应用鉴定装置 8 与应用鉴定功能 3 之间进行鉴定，但是该鉴定是不成功的。接着，假定当前运行的应用软件的许可类别是 A。此时，由于该应用软件是一种执行显示的软件，因而在应用鉴定装置 8 与应用鉴定功能 3 之间的鉴定将会成功完成。

而当 AV 数据禁止拷贝时，如果应用软件是带有许可 C 的软件，则鉴定将会成功完成。图 7 示出对 AV 数据的使用允许状态、应用软件的许可类别和鉴定的成功/失败状态间关系编制的表。当应用软件部分 13 和系统部分 12 之间成功完成鉴定时，传送解密装置 6 从传送鉴定装置 2 接收解密密钥并对经 1394 D－IF 1 接收到的 AV 数据进行解密。接着，PC 内部加密装置 7 对该 AV 数据重新加密。在 PC 24 中，版权保护的 AV 数据以加密形式传送，直到应用软件将其提供应用为止。数据使用(解码和显示)装置 10 中的解密装置 11 从应用鉴定装置 8 接收解密密钥并对 AV 数据解密。解密后的 AV 数据从数据使用(解码和显示)装置 10 传送到当前运行的应用软件用于处理。

另一方面，应用软件部分 13 与系统部分 12 间的鉴定不成功，则 AV 数据一旦被传送解密装置 6 解密就再次被 PC 内部加密装置 7 加密，加密后的数据传送到数据使用(解码和显示)装置 10。由于鉴定失败，所以应用鉴定装置 8 不能从应用鉴定功能 3 接收解密密钥；结果，解密密钥不能传送到解密装置 11，因此，不能对 AV 数据解密。在这种情况下，如果应用软件没有合适的许可，则由于鉴定失败，该应用软件不能够解密 AV 数据进行处理。

在这种情况下，版权保护的 AV 数据在 PC 24 内加密，并在系统部分 12 与应用软件部分 13 间进行鉴定，有选择地识别具有合适许可的应用软件；因此，如果没有合适许可的应用软件接收 AV 数据，则由于数据被加密，故该应用软件不能将 AV 数据作为有效数据进行处理，因而版权保护的 AV 数据能得到保护。

本发明的重新加密可用与发送加密数据用密钥相同的密钥或不同的密钥。而且，以加密形式接收到的 AV 数据可以在 PC 内以该加密形式传送，而不对其进行一次解密。还应看到，重新(再次)加密的方法不限定于上面描述的特定方法，任何其它规定的方法都可使用。

此外，在本实施例中，按照系统部分与应用软件部分间鉴定失败时发送加密数据到数据使用(解码和显示)装置，对 PC 内部加密装置进行了描述，但是当鉴定失败时可代替发送如蓝色背景屏等无效数据到数据使用(解码和显示)装置。这样，

AV 数据的版权能得到更安全的保护。

本发明的系统部分可用构成 1393 D—IF 的硬件构成，或用如驱动器或 OS 的系统软件构成。也就是说，它可用 PC 中的硬件构成或用系统软件构成。

而且，本实施例的许可不限定于如上所述的分成 3 类 A、B、C 的一种分类。它可以分成 4 类或 2 类，唯一的要求是根据 AV 数据的版权状态进行分类。

本实施例虽然取 STB 为外部装置、PC 从其接收版权保护的 AV 数据作为例子进行了描述，但本发明不限定于该特定的例子；也即，任何其它装置，如 DVC、DVHS、HDD、DVD—RAM 或广播接收机等，只要能发送版权保护的 AV 数据，都可以用作外部装置。

本实施例虽然取 IEEE 1394 作为例子进行了描述，但是，本发明不限定于该特定的例子，任何其它网络，只要具有发送版权保护的 AV 数据及它的版权信息，都可使用。

还应当看到，本实施例的 AV 数据不限定于上面描述的视频/音频数据，还应当理解为包含如版权保护的程序、文件或版权保护的任何其它数据。

本实施例中描述的 PC 只不过是本发明计算机的一个例子。

(实施例 2)

下面，参照图 2 描述第 2 实施例。

本实施例的描述涉及的情况是，在执行系统部分与应用软件部分间鉴定之前，使用区分非法或合法应用软件的管理标准(management criterion)(下文称为 CRL)对应用软件进行区分。

与第 1 实施例的区别在于，系统部分 12 包含 CRL 存储器 14，应用 CRL 存储器 15，和 CRL 比较装置 16。下面的描述将集中在与第 1 实施例的差别上。

CRL 存储器 14 是一种存储区分非法或合法装置用管理标准的存储器。应用 CRL 存储器 15 是一种存储区分非法或合法软件用管理标准的装置。CRL 比较装置 16 是一种根据 CRL 判别应用软件是非法还是合法的装置。

下面将描述具有上述结构的本实施例的运作。

在该实施例中，也假定 AV 数据从 STB 发送，且该 AV 数据是版权保护的数据。首先，在传送解密装置 6 与 STB 间进行鉴定之前，利用存储在 STB 的 CRL 存储器中的 CRL 判别 PC 24 是否为合法装置。如果判别为合法装置，则传送鉴定装置 2 与 STB 进行鉴定。如果判别为非法装置，则 STB 不进行鉴定，对加密过的 AV 数据解密用的密钥不传送到 PC 24。

这里，假定 PC 24 被 STB 判别为合法装置。那么传送鉴定装置 2 经 1394 D—IF 1 与 STB 进行鉴定。当鉴定成功完成时，STB 经 1394 D—IF 1 传送解密 AV 数据用的密钥到传送鉴定装置 2。

接着，签名产生装置 9 为当前运行的应用软件产生数字签名，该数字签名存储在签名存储器 4 中。CRL 比较装置 16 将存储在签名存储器 4 中的数字签名的内容与应用 CRL 存储器 15 中的内容进行比较，判别当前运行的应用软件是非法软件还是合法软件。如果是非法软件，则不进行应用软件部分 13 与系统部分 12 间的鉴定。相反，若是合法软件，则接着执行应用软件部分 13 与系统部分 12 间的鉴定。这里，假定许可类同于第 1 实施例中描述的，并附加于应用软件。

应用 CRL 存储器 15 是一种常驻在 PC 24 中的 OS 或驱动器存储器；可预先存储分开产生的 CRL，或可采用从 IEEE 1394 传送来的 CRL。通常，CRL 不固定，但是可根据情况加以更新。例如，如果装置或应用改变到对版权侵权并流传开，则可识别这种装置或应用，由此更新 CRL，使得鉴定不成功。当应用软件部分 13 与系统部分 12 间成功完成鉴定时，传送解密装置 6 从传送鉴定装置 2 接收解密密钥，并对经 1394 D—IF 接收到的 AV 数据解密。接着，PC 内部加密装置 7 对 AV 数据再(重新)加密。在 PC 24 中，版权保护的 AV 数据以加密形式传送，直到由应用软件提供使用为止。数据使用(解码和显示)装置 10 从应用鉴定装置 8 接收解密密钥，并解密 AV 数据。解密后的 AV 数据从数据使用(解码和显示)装置 10 传送到当前运行的软件，用于处理。

相反，当应用软件部分 13 与系统部分 12 间鉴定失败时，AV 数据一旦由传送解密装置 6 解密，那么就再由 PC 内部加密装置 7 加密，加密后的数据传送到数据使用(解码和显示)装置 10。由于鉴定失败，应用鉴定装置 8 不能够将解密密钥传送到解密装置 11，因此，不能够对 AV 数据解密。在这种情况下，由于鉴定失败，故不能够对 AV 数据解密，用于处理。

或者从应用 CRL 存储器 15 检索一攻破和无效的防止篡改系统的版本信息，并且如果该应用的版本是无效的防止篡改系统的版本，那么解密 AV 数据的密钥不传送到应用鉴定功能 3，应用软件部分 13 与系统部分 12 间也不执行鉴定。

在这种情况下，在应用软件部分与系统部分间执行鉴定之前，利用 CRL 判别当前运行的应用软件是非法的还是合法的，如果存在对版权保护的 AV 数据执行非法操作的潜在危险，则能预先拒绝该应用软件。

本发明的重新加密可使用与发送数据加密用的相同的密钥或不同的密钥。以

加密形式接收到的 AV 数据可在 PC 中以该加密形式传送，一次也不对其解密。还应当看到，重新(再次)加密的方法不限定于上面描述的特定方法，任何其它规定的方法都可使用。

此外，在本实施例中，按照系统部分与应用软件部分间鉴定失败时发送加密数据到数据使用(解码和显示)装置，对 PC 内部加密装置进行了描述，但是当鉴定失败时可代替发送如蓝色背景屏(blueback screen)等无效数据到数据使用(解码和显示)装置。这样，AV 数据的版权能得到更安全的保护。

本发明的系统部分可用构成 1393 D－IF 的硬件构成，或用如驱动器或 OS 的系统软件构成。也就是说，它可用 PC 中的硬件构成或用系统软件构成。

本实施例虽然取 STB 为外部装置、PC 从其接收版权保护的 AV 数据作为例子进行了描述，但本发明不限定于该特定的例子；也即，任何其它装置，如 DVC、DVHS、HDD、DVD－RAM 或广播接收机等，只要能发送版权保护的 AV 数据，都可以用作外部装置。

本实施例虽然取 IEEE 1394 作为例子进行了描述，但是，本发明不限定于该特定的例子，任何其它网络，只要具有发送版权保护的 AV 数据及它的版权信息，都可使用。

还应当看到，本实施例的 AV 数据不限定于上面描述的视频/音频数据，还应当理解为包含如版权保护的程序、文件或版权保护的任何其它数据。

本实施例中描述的 PC 只不过是本发明计算机的一个例子。

(实施例 3)

下面，参照图 3 描述第 3 实施例。

本实施例的描述涉及的情况是，使用篡改鉴定功能，判别应用软件是否被非法改变。

与第 1 实施例的区别在于，系统部分 12 包含篡改鉴定功能 17，应用软件部分 13 包含软件检查装置 18。

篡改鉴定功能 17 是一种验证应用软件产生的篡改码以便确定应用软件是否已被篡改的装置。软件检查装置 18 是一种检查当前运行应用和产生篡改码的装置。

下面将描述具有上述结构的本实施例的运作。

如上所述，产生篡改码的防篡改软件涉及具有防止内部分析或改变的软件。也即，所涉及的软件能防止意志欠佳的人企图非法使用版权保护的 AV 数据的犯罪

行为。防篡改软件产生一个称为篡改码的码。软件检查装置 18 检查程序，验证是否存在篡改，也检查执行环境，验证沿数据通道是否存在拦截，存在第 3 方监听程序的执行等。篡改码是表示这种验证结果或中间结果的数据。通过验证该篡改码，能确定防篡改软件是否已遭篡改。也即，在本实施例中，应用软件装有内置的防篡改系统。

这里，如第 1 实施例中那样，假定鉴定在 STB 与传送鉴定装置 2 间进行，并且鉴定成功完成。于是，软件检查装置 18 检查当前运行的应用软件并产生篡改码。所产生的篡改码传送到应用鉴定装置，在这里，篡改码通过签名产生装置 9 写入数字签名；然后，该数字签名存储在签名存储器 4 中。通过参照存储在签名存储器 4 中的数字签名，篡改鉴定功能 17 检索当前运行的应用软件的篡改码，对其进行验证，并向应用鉴定功能 3 报告当前运行的应用软件是否被非法改变或是否在拦截数据或监听程序执行的验证结果。为简单起见，下面的描述是假定，是否应用被非法改变的验证包含是否进行拦截数据或监听程序的验证。如果应用软件非法改变，则应用鉴定功能 3 不将解密 AV 数据的密钥传送到应用鉴定装置 8，也不

进行应用软件部分 13 与系统部分 12 间的鉴定。如果应用软件未非法改变，则应用鉴定功能 3 和应用鉴定装置 8 根据记录在签名存储器 4 中的数字签名执行鉴定。这里，如第 1 实施例中那样，许可附加于应用软件。当鉴定成功完成时，应用鉴定功能 3 将解密 AV 数据的密钥传送到应用鉴定装置 8。

当应用软件部分 13 与系统部分 12 间成功完成鉴定时，传送解密装置 6 从传送鉴定装置 2 接收解密密钥，并对经 1394 D—IF 1 接收到的 AV 数据解密。接着，PC 内部加密装置 7 对 AV 数据再(重新)加密。在 PC 24 中，版权保护的 AV 数据以加密形式传送，直到由应用软件提供使用为止。构成数据使用(解码和显示)装置 10 的解密装置 11 从应用鉴定装置 8 接收解密密钥，并解密 AV 数据。解密后的 AV 数据从数据使用(解码和显示)装置 10 传送到当前运行的软件，用于处理。

相反，当应用软件部分 13 与系统部分 12 间鉴定失败时，AV 数据一旦由传送解密装置 6 解密，那么就再由 PC 内部加密装置 7 加密，加密后的数据传送到数据使用(解码和显示)装置 10。由于鉴定失败，应用鉴定装置 8 不能够将解密密钥传送到解密装置 11，因此，不能够对 AV 数据解密。在这种情况下，如果应用软件没有适当的许可，则由于鉴定失败，故不能够处理 AV 数据。

在这种情况下，通过将防篡改系统结合到应用软件并增加检查非法篡改的应用软件的功能，从而使 AV 数据的版权能保护得更安全。

本发明的重新加密可使用与发送数据加密用的相同的密钥或不同的密钥。而且，以加密形式传输的AV数据可在PC中以该加密形式传送，一次也不对其解密。还应当看到，重新(再次)加密的方法不限定于上面描述的特定方法，任何其它规定的方法都可使用。

此外，在本实施例中，按照系统部分与应用软件部分间鉴定失败时发送加密数据到数据使用(解码和显示)装置，对PC内部加密装置进行了描述，但是可代替使用PC内部加密装置，当鉴定失败时发送如蓝色背景屏等无效数据到数据使用(解码和显示)装置。这样，AV数据的版权能得到更安全的保护。

本发明的系统部分可用构成1393 D—IF的硬件构成，或用如驱动器或OS的系统软件构成。也就是说，它可用PC中的硬件构成或用系统软件构成。

本实施例虽然取STB为外部装置、PC从其接收版权保护的AV数据作为例子进行了描述，但本发明不限定于该特定的例子；也即，任何其它装置，如DVC、DVHS、HDD、DVD—RAM或广播接收机等，只要能发送版权保护的AV数据，都可以用作外部装置。

本实施例虽然取IEEE 1394作为例子进行了描述，但是，本发明不限定于该特定的例子，任何其它网络，只要具有发送版权保护的AV数据及它的版权信息，都可使用。

还应当看到，本实施例的AV数据不限定于上面描述的视频/音频数据，还应当理解为包含如版权保护的程序、文件或版权保护的任何其它数据。

而且，本发明的篡改码和防篡改验证功能不限定于使用特定的防篡改系统，也可用所需要的任何防篡改系统构成。

本实施例中描述的PC只不过是本发明计算机的一个例子，本实施例的篡改鉴定功能只不过是本发明防篡改验证功能的一个例子。

(实施例4)

下面，参照图4描述第4实施例。

本实施例的描述涉及的情况是，使用篡改鉴定功能，判别应用软件是否被非法改变。

与第3实施例的区别在于，系统部分12包含多个篡改鉴定功能21和版本选择装置20，应用软件部分13中的软件检查装置19不仅产生篡改码，而且还产生类型信息，表明建立在应用软件的防篡改系统的类型。

版本选择装置20是一种根据记录在签名存储器4中的数字签名选择对应防

篡改系统的篡改鉴定功能的装置。

下面将描述具有上述结构的本实施例的运作。

如第 3 实施例中那样，这里假设应用软件装有内置的防篡改系统，并假定鉴定在 STB 与传送鉴定装置 2 间进行。假定鉴定成功完成。于是，软件检查装置 19 检查当前运行的应用软件并产生篡改码和表明内置防篡改系统类型的类型信息。所产生的篡改码类型信息传送到应用鉴定装置 8，在这里，篡改码和类型信息通过签名产生装置 9 写入数字签名；然后，该数字签名存储在签名存储器 4 中。版本选择装置 20 通过参照存储在签名存储器 4 中的防篡改系统类型信息选择要使用的篡改鉴定功能。这里假定版本选择装置 20 包含它自身的用于篡改版本的 CRL 存储器(未图示)，通过使用该 CRL 存储器，版本选择装置 20 工作，以便不选择已知该方法失败的防篡改检查装置 19。通过参照存储在签名存储器 4 中的数字签名，所选篡改鉴定功能 21 检索当前运行的应用软件的篡改码并对其进行验证。并向应用鉴定功能 3 报告当前运行的应用软件是否被非法改变的验证结果。如果应用软件非法改变，则应用鉴定功能 3 不将解密 AV 数据的密钥传送到应用鉴定装置 8，也不进行应用软件部分 13 与系统部分 12 间的鉴定。如果应用软件未非法改变，则应用鉴定功能 3 和应用鉴定装置 8 根据记录在签名存储器 4 中的数字签名执行鉴定。这里，如在第 1 实施例中那样，许可附加于应用软件。当鉴定成功完成，应用鉴定功能 3 将解密 AV 数据的密钥传送到应用鉴定装置 8。

当应用软件部分 13 与系统部分 12 间成功完成鉴定时，传送解密装置 6 从传送鉴定装置 2 接收解密密钥，并对经 1394 D—IF 1 接收到的 AV 数据解密。接着，PC 内部加密装置 7 对 AV 数据再(重新)加密。在 PC 24 中，版权保护的 AV 数据以加密形式传送，直到由应用软件提供使用为止。数据使用(解码和显示)装置 10 中的解密装置 11 从应用鉴定装置 8 接收解密密钥，并解密 AV 数据。解密后的 AV 数据从数据使用(解码和显示)装置 10 传送到当前运行的软件，用于处理。

相反，当应用软件部分 13 与系统部分 12 间鉴定失败时，AV 数据一旦由传送解密装置 6 解密，那么就再由 PC 内部加密装置 7 加密，加密后的数据传送到数据使用(解码和显示)装置 10。由于鉴定失败，应用鉴定装置 8 不能够将解密密钥传送到解密装置 11，因此，不能够对 AV 数据解密。在这种情况下，如果应用软件没有适当的许可，则由于鉴定失败，故不能够解密 AV 数据，进行处理。

在这种情况下，通过不仅将防篡改系统结合到应用软件而且还在系统部分中提供多个防篡改鉴定功能，如果应用软件的防篡改系统失败，则系统部分只要转

接到另一种防篡改鉴定功能，消除了更新 OS 等版本的要求，而且当防篡改系统失败时，能将损害减到最小。

本发明的重新加密可使用与发送数据加密用的相同的密钥或不同的密钥。而且，以加密形式传输的 AV 数据可在 PC 中以该加密形式传送，一次也不对其解密。还应当看到，重新(再次)加密的方法不限定于上面描述的特定方法，任何其它规定的方法都可使用。

此外，在本实施例中，按照系统部分与应用软件部分间鉴定失败时发送加密数据到数据使用(解码和显示)装置，对 PC 内部加密装置进行了描述，但是可代替为，当鉴定失败时发送如蓝色背景屏等无效数据到数据使用(解码和显示)装置。这样，AV 数据的版权能得到更安全的保护。

本发明的系统部分可用构成 1393 D－IF 的硬件构成，或用如驱动器或 OS 的系统软件构成。也就是说，它可用 PC 中的硬件构成或用系统软件构成。

本实施例虽然取 STB 为外部装置、PC 从其接收版权保护的 AV 数据作为例子进行了描述，但本发明不限定于该特定的例子；也即，任何其它装置，如 DVC、DVHS、HDD、DVD－RAM 或广播接收机等，只要能发送版权保护的 AV 数据，都可以用作外部装置。

本实施例虽然取 IEEE 1394 作为例子进行了描述，但是，本发明不限定于该特定的例子，任何其它网络，只要具有发送版权保护的 AV 数据及它的版权信息，都可使用。

还应当看到，本实施例的 AV 数据不限定于上面描述的视频/音频数据，还应当理解为包含如版权保护的程序、文件或版权保护的任何其它数据。

而且，本发明的篡改码和防篡改验证功能不限定于使用如上所述特定的防篡改系统，也可用所需要的任何防篡改系统构成。

本实施例中描述的 PC 只不过是本发明计算机的一个例子，本实施例的篡改鉴定功能只不过是本发明防篡改验证功能的一个例子。

(实施例 5)

下面，参照图 5 描述第 5 实施例。

该实施例的描述涉及的情况是，用于处理 AV 数据的应用软件相关的信息利用电子水印嵌入 AV 数据。

电子水印是按难以改变的方式将签名等数据插入到 AV 数据的技术，不管该技术是根据模拟数据叠印还是根据数字密码术。

与第 1 和第 2 实施例的区别是，系统部分包含签名嵌入装置 22 和电子水印嵌入装置 23。

签名嵌入装置 22 参照记录在签名存储器 4 中的数字签名，进行选择电子水印嵌入装置 23 所需信息、准备格式等电子水印嵌入装置 23 的预处理。电子水印嵌入装置 23 按照签名嵌入装置 22 准备的格式将电子水印产生数据嵌入 AV 数据。

在该实施例中，传送鉴定装置 2，应用鉴定功能 3，签名存储器 4，应用鉴定装置 8，签名产生装置 9，传送解密装置 6，PC 内部加密装置 7，数据使用(解码和显示)装置 10，和解密装置 11 与实施例 1 中对应的构件相同。CRL 比较装置 16 与第 2 实施例中对应的构件相同。

下面，将描述具有上述结构的本实施例的运作。

假定在外部装置，如 STB 与传送鉴定装置 2 之间进行鉴定并获得成功。也假定在应用鉴定装置 8 与应用鉴定功能 3 之间成功完成鉴定。于是，利用传送解密装置 6 对经 1394 D－IF 1 输入的加密 AV 数据进行解密。签名嵌入装置 22 从签名存储器 4 检索包含应用软件信息的数字签名，并选择其内容。所选内容包含应用软件的名称，应用软件的版本号，关于用户的信息，和关于 AV 数据本身的信息。签名嵌入装置 22 将例如准备格式等预先处理加给这些信息，并将处理后的信息发送给电子水印嵌入装置 23。电子水印嵌入装置 23 通过将这些信息结合到解密后的 AV 数据中，产生电子水印。AV 数据与由此结合在其中的电子水印，再次由 PC 内部加密装置 7 加密，加密后的 AV 数据传送到数据使用(解码和显示)装置 10。解密装置 11 对 AV 数据解密，而数据使用(解码和显示)装置 10 将其传送到当前运行的应用软件。接收到 AV 数据的应用软件执行如显示、记录、再现等处理。

这里假定应用软件非法记录施以电子水印的 AV 数据并在 PC 24 外流传。也假定包含在非法流传的 AV 数据中的 CGMS 或 EMI 被非法应用改变。于是，被非法改变后的 AV 数据现在也可记录在合法的装置上，并且流传到许多装置。如果检查 AV 数据非法流传的监督组织获得该 AV 数据，则该组织通过参照嵌入该 AV 数据中的电子水印能检索到下面的信息。也就是说，从与 AV 数据相关的信息可发现该 AV 数据是禁止拷贝的数据等，并从与应用软件相关的信息能识别用于非法拷贝和流传该 AV 数据的源应用软件。

在这种情况下，本发明能识别非法流传的源；此外，由于本发明的计算机备有更新 CRL 的装置，因而根据与源有关的信息更新 CRL，就能将负有非法流传责任的应用排除在使用 AV 数据之外，据此，提供防止非法的特定的装置。按照该方

法，通过使用电子水印，能识别非法拷贝的源，因而能很容易隔离非法应用软件。

电子水印系统不限定于本实施例中使用的，任何其它系统，只要能将上面提到的信息正确地嵌入 AV 数据并在按规定格式解码前或后能正确地提取该信息，都可以使用。

按照上述方式，通过将电子水印嵌入 AV 数据，能够很容易地隔离或拒绝非法应用软件。

(实施例 6)

下面，参照图 6 描述第 6 实施例。

本实施例的 PC 组合第 1 到第 5 实施例中描述的 PC 的所有功能。

传送鉴定装置 2，应用鉴定功能 3，签名存储器 4，应用鉴定装置 8，签名产生装置 9，传送解密装置 6，PC 内部加密装置 7，数据使用(解码和显示)装置 10，和解密装置 11 与第 1 实施例中对应的相同。CRL 存储器 14，应用 CRL 存储器 15，和 CRL 比较装置 16 与第 2 实施例中描述的对应构件相同。版本选择装置 20 和篡改鉴定装置 21 与第 4 实施例中描述的对应构件相同。签名嵌入装置 22 和电子水印嵌入装置 23 与第 5 实施例中描述的对应构件相同。

上述构成结合了第 1 至第 5 实施例中描述的全部功能，而且还备有根据防篡改系统检查软件可靠性的装置，根据电子水印检测非法使用的可靠的检测方法，和一旦检测到就防止非法使用再现的装置；因此，能按可靠的方式防止非法使用版权保护的 AV 数据，而且由于将版本概念引入防篡改系统，能将非法使用产生的间接损害减到最小。

也可以按程序记录媒体的形式嵌入本发明，程序和/或数据记录在该媒体，使计算机能执行上面任一实施例中描述的全部或部分本发明的全部或部分功能，其中，程序和/或数据是计算机可读的，且计算机读出的程序和/或数据用来与该计算机协作执行上述功能。

术语“数据”这里包含数据结构，数据格式，和数据类型。

术语“媒体”是指如 ROM 的录媒体，如英特网的传送媒体，或如光、电波、声波等的传送媒体。

术语“保持媒体”是指，例如，具有记录在其上的程序和/或数据的记录媒体，或传送程序和/或数据的传送媒体等。

术语“计算机可处理”是指，例如，在如 ROM 的记录媒体情况下，计算机可读该媒体，在传送媒体情况下，要传送的程序和/或数据能由计算机处理，作为传

送的结果。

术语“信息集”包含，例如，像程序和/或数据那样的软件。

工业上的可应用性

从以上说明清楚可见，本发明所提供的计算机和程序记录媒体，能确保应用软件保护授予版权数据的版权，能寻找非法改变的应用软件，识别和拒绝非法应用软件，并能防止非法流传而不需额外的费用。

说 明 书 附 图

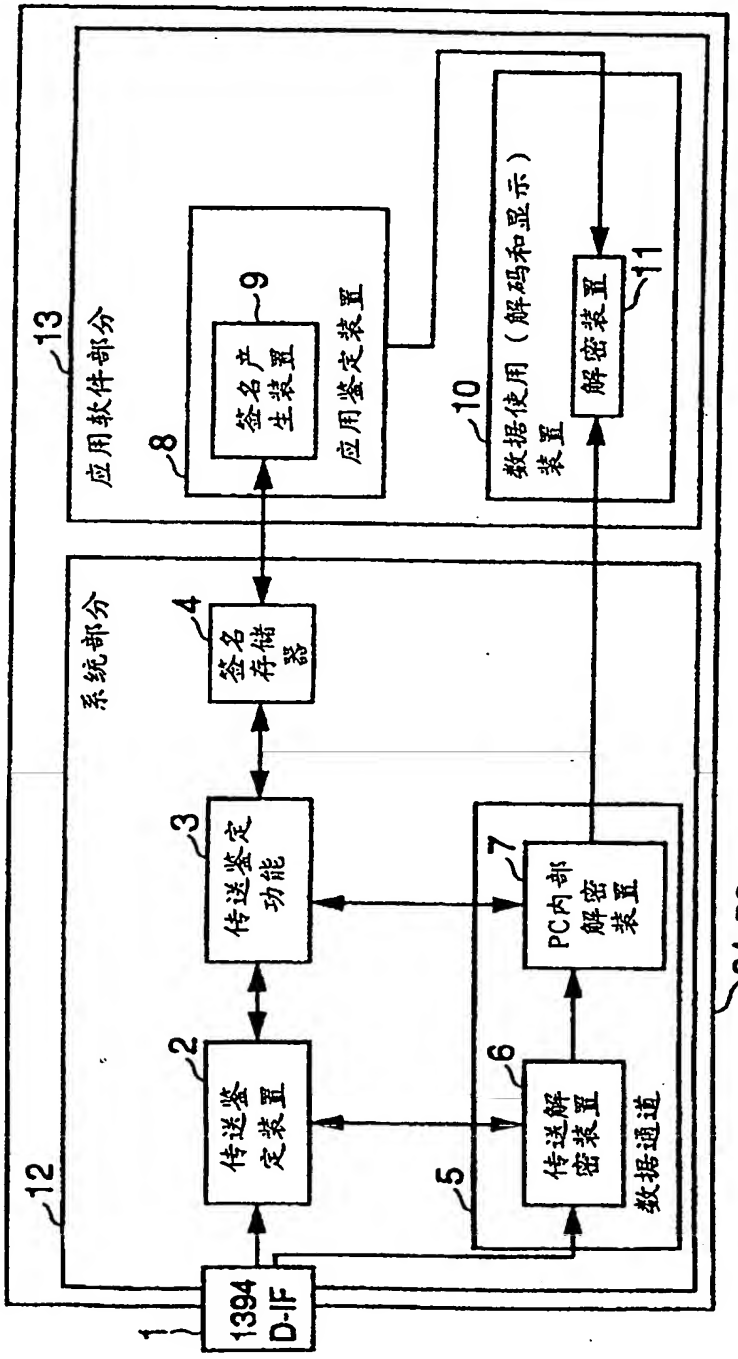

1394 D-IF
1
12
系统部分
传送鉴定装置
2
传送鉴定功能
3
签名存储器
4
5
传送解密装置
6
PC内部解密装置
7
数据通道
24 PC
13
应用软件部分
8
应用鉴定装置
签名产生装置
9
10
数据使用（解码和显示）装置
解密装置
11

图 1

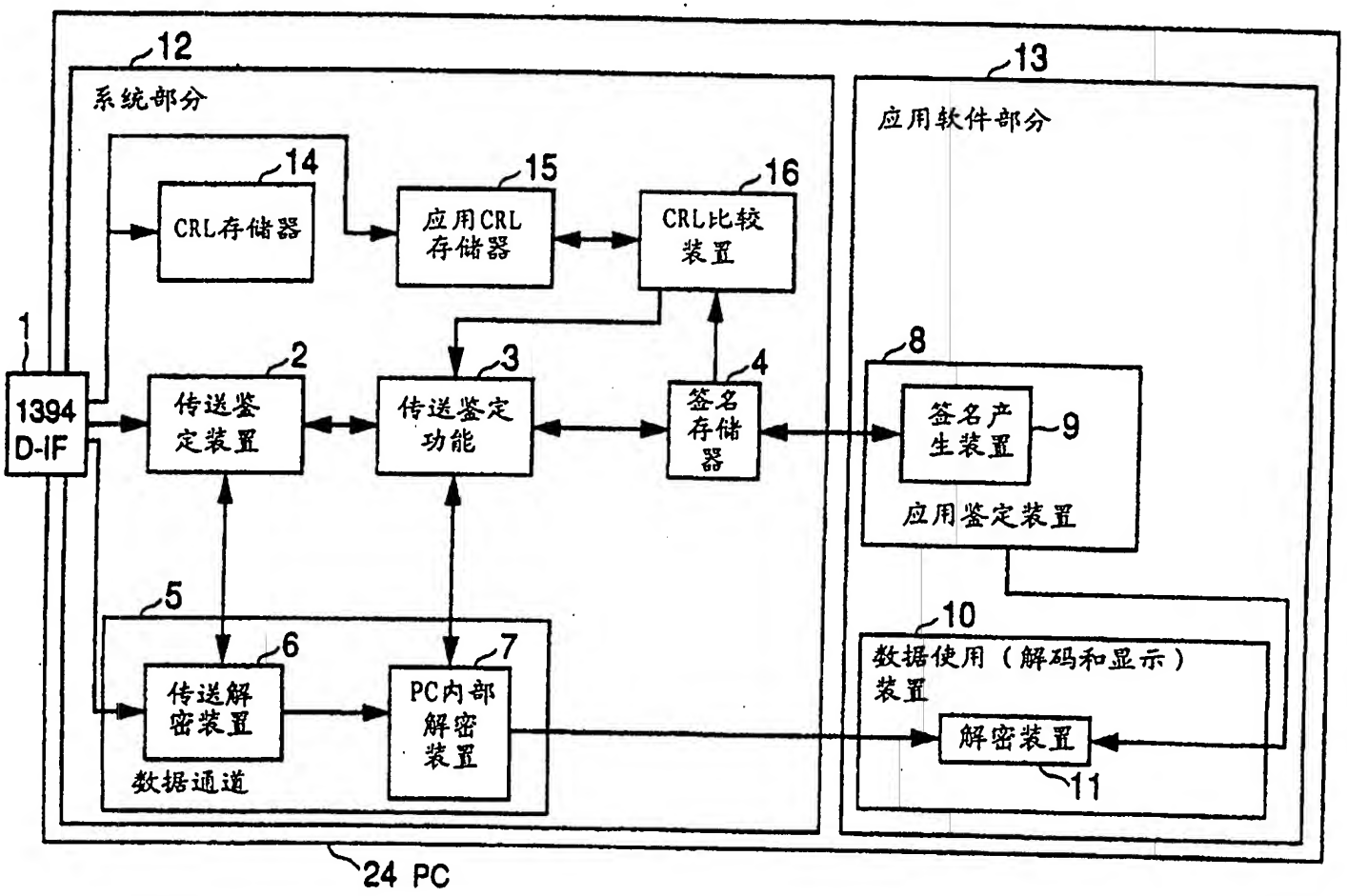

12
系统部分
13
应用软件部分
14
CRL存储器
15
应用CRL
存储器
16
CRL比较
装置
1
1394
D-IF
2
传送鉴
定装置
3
传送鉴定
功能
4
签名
存储
器
8
签名产
生装置
9
应用鉴定装置
5
6
传送解
密装置
7
PC内部
解密
装置
数据通道
10
数据使用（解码和显示）
装置
解密装置
11
24 PC

图 2

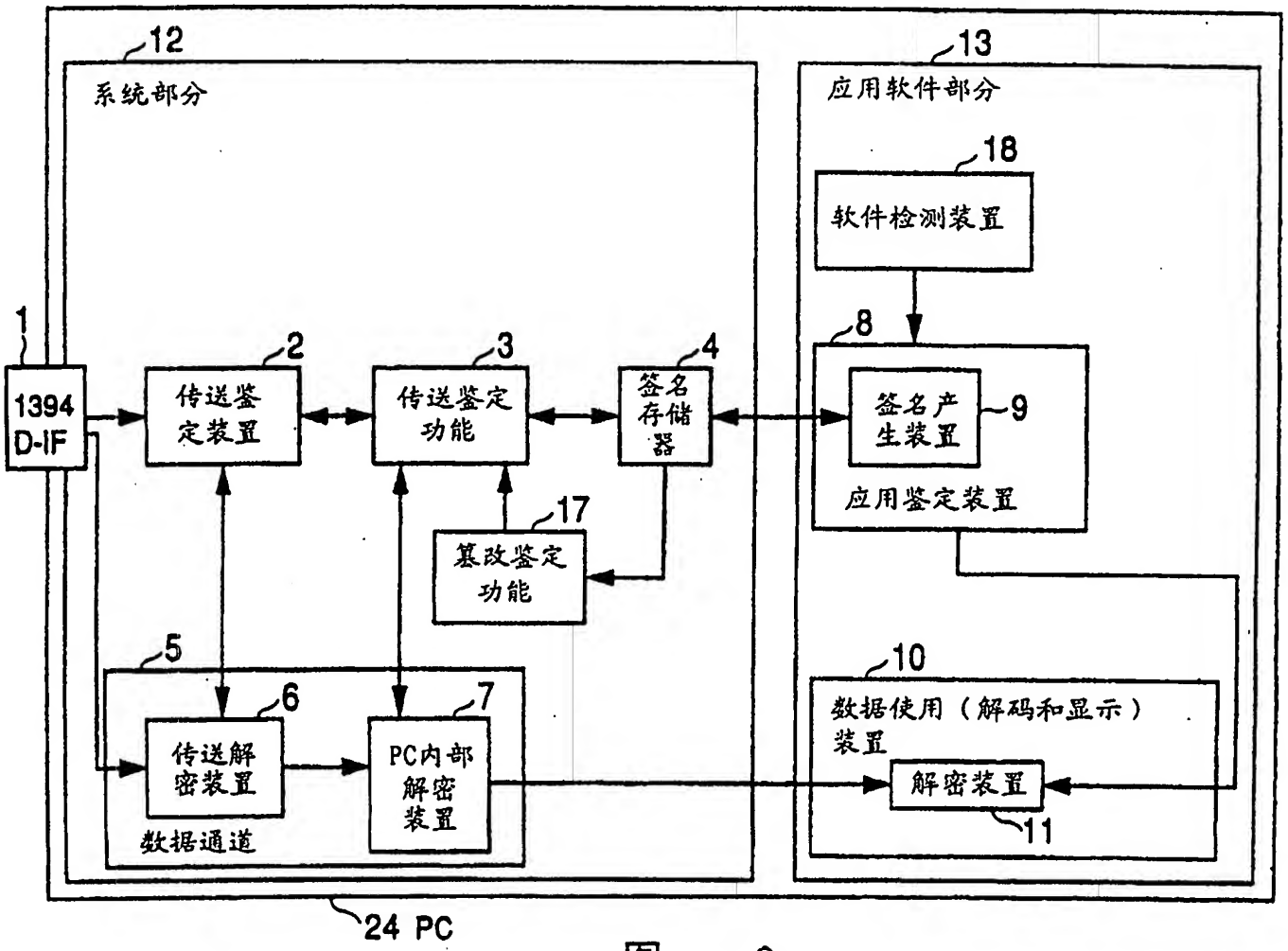

12
系统部分
13
应用软件部分
18
软件检测装置
1
1394
D-IF
2
传送鉴
定装置
3
传送鉴定
功能
4
签名
存储
器
8
签名产
生装置
9
应用鉴定装置
17
篡改鉴定
功能
5
6
传送解
密装置
7
PC内部
解密
装置
数据通道
10
数据使用（解码和显示）
装置
解密装置
11
24 PC

图 3

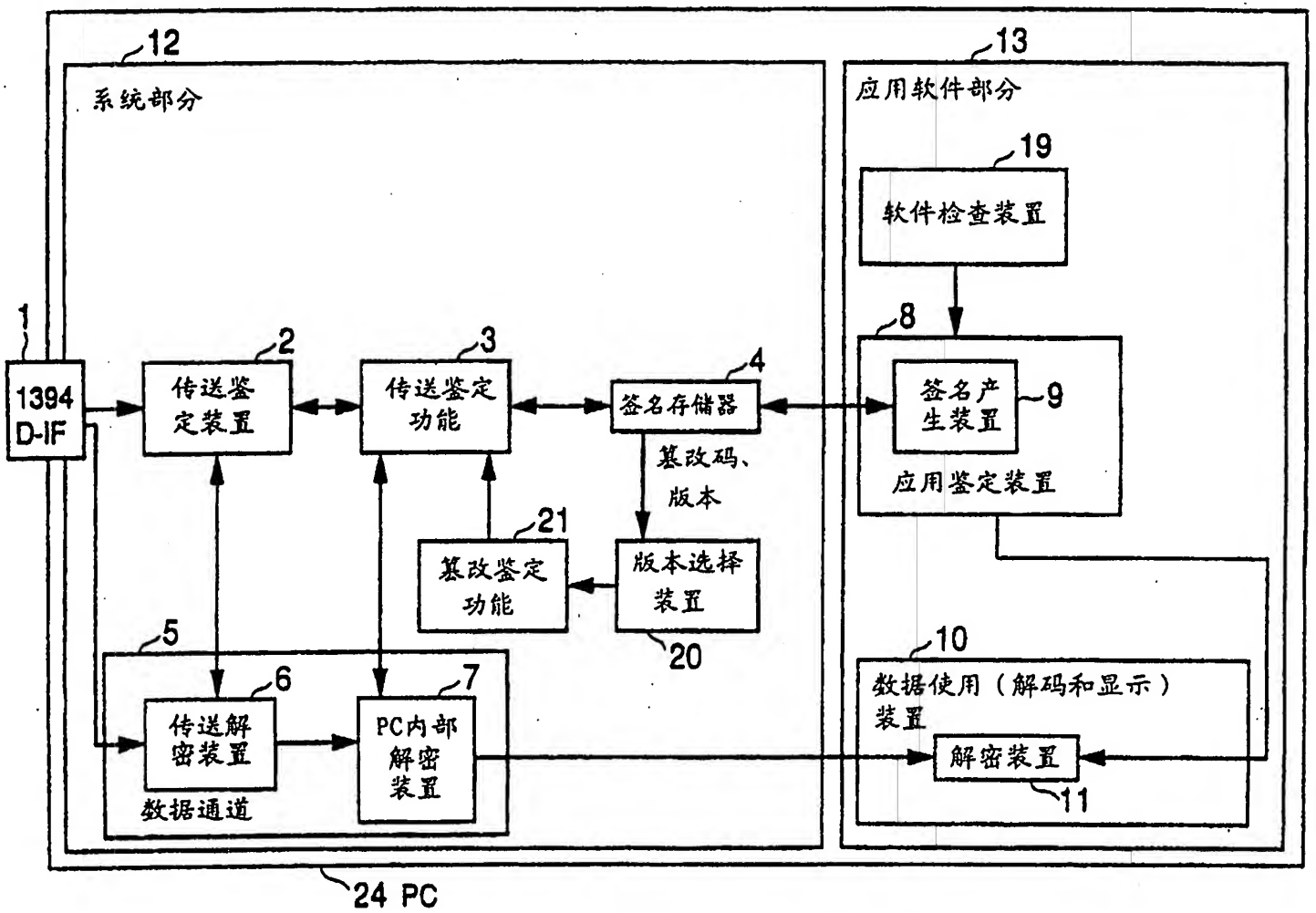

12
系统部分
13
应用软件部分
19
软件检查装置
1
1394
D-IF
2
传送鉴
定装置
3
传送鉴定
功能
4
签名存储器
8
签名产
生装置
9
应用鉴定装置
篡改码、
版本
21
篡改鉴定
功能
版本选择
装置
20
5
6
传送解
密装置
7
PC内部
解密
装置
数据通道
10
数据使用（解码和显示）
装置
解密装置
11
24 PC

图 4

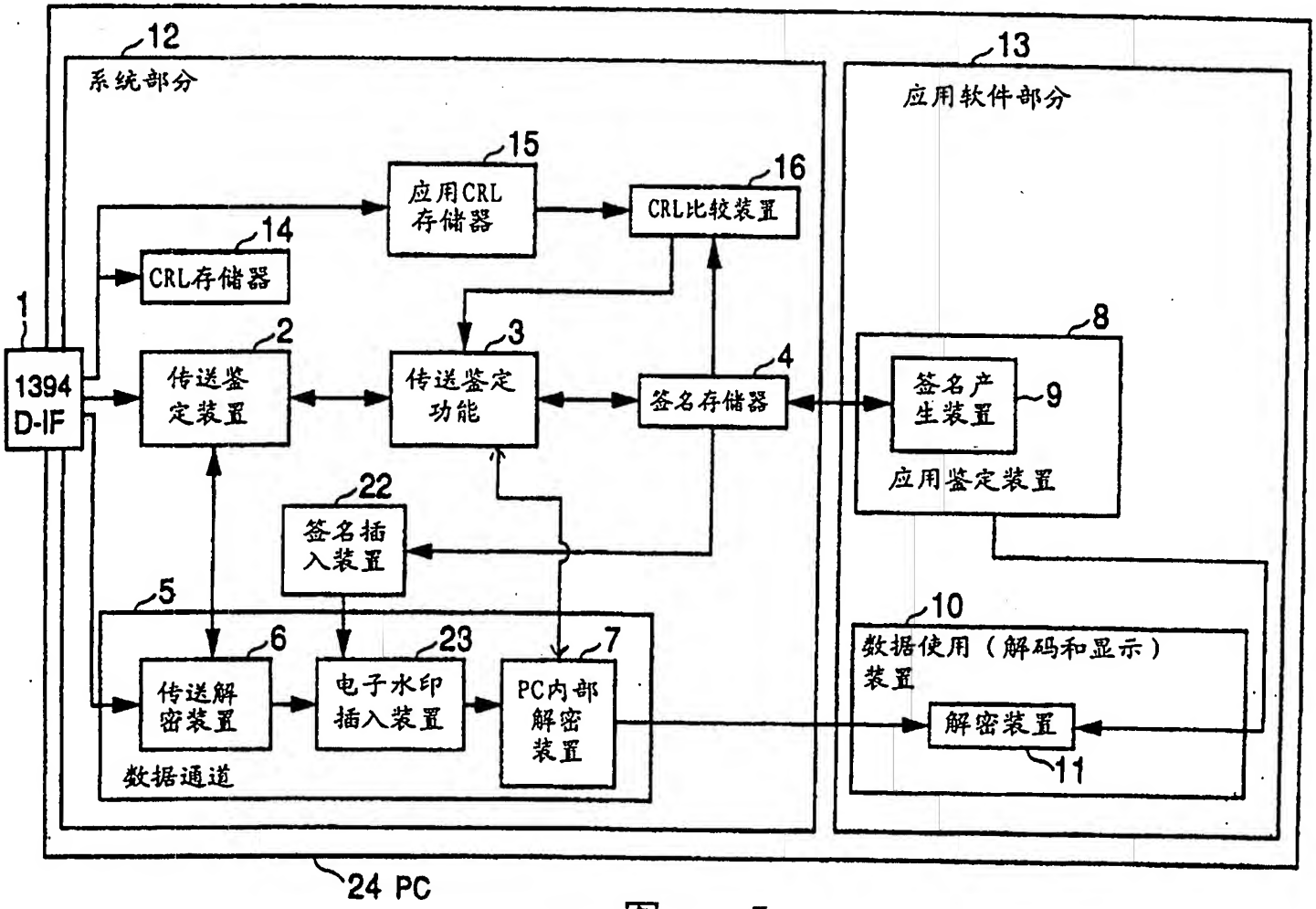

12
系统部分
13
应用软件部分
15
应用CRL
存储器
16
CRL比较装置
14
CRL存储器
1
1394
D-IF
2
传送鉴
定装置
3
传送鉴定
功能
4
签名存储器
8
签名产
生装置
9
应用鉴定装置
22
签名插
入装置
5
6
23
7
传送解
密装置
电子水印
插入装置
PC内部
解密
装置
数据通道
10
数据使用（解码和显示）
装置
解密装置
11
24 PC

图 5

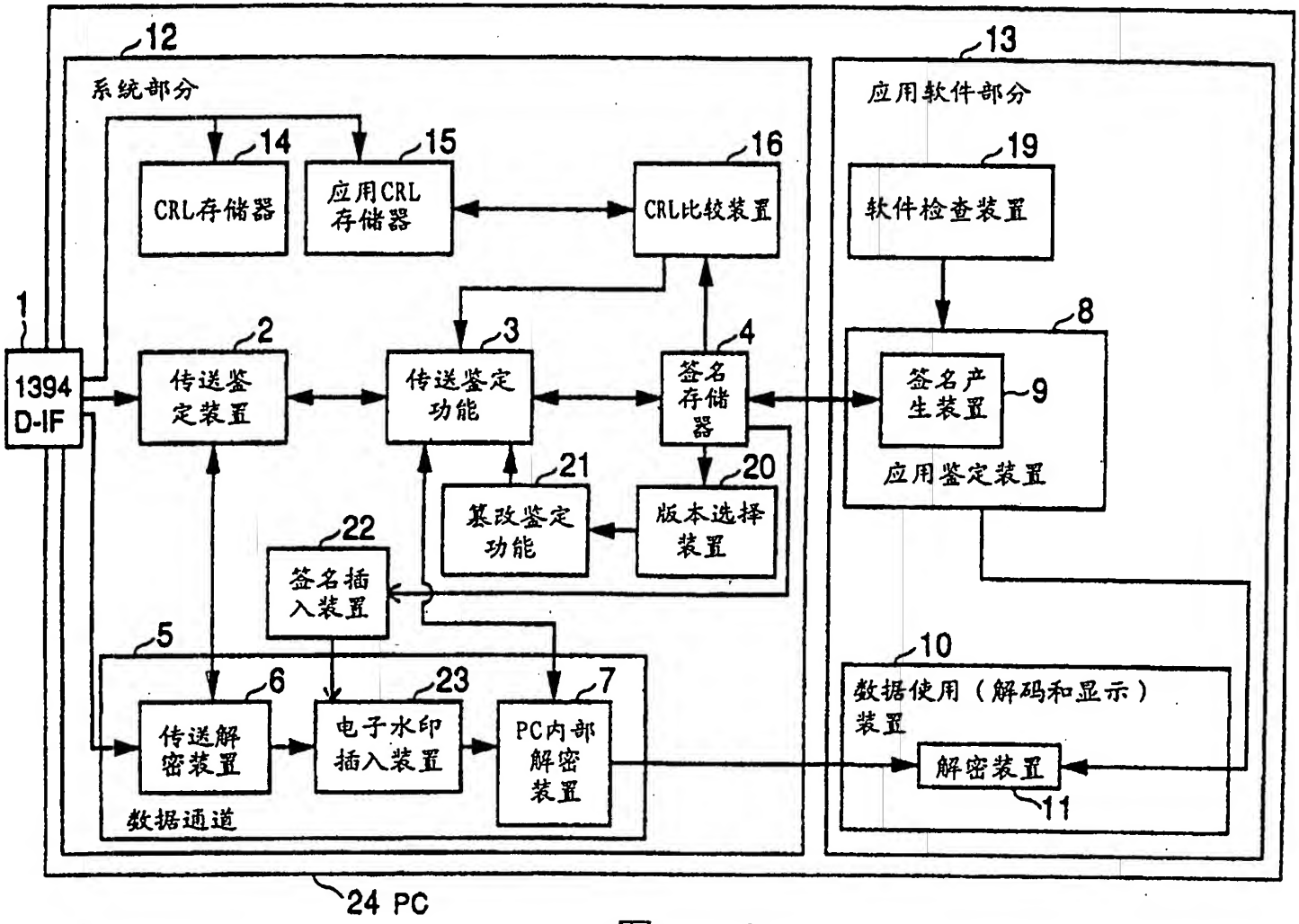

12
系统部分
13
应用软件部分
14
CRL存储器
15
应用CRL
存储器
16
CRL比较装置
19
软件检查装置
1
1394
D-IF
2
传送鉴
定装置
3
传送鉴定
功能
4
签名
存储
器
8
签名产
生装置
9
应用鉴定装置
21
篡改鉴定
功能
20
版本选择
装置
22
签名插
入装置
5
10
数据使用（解码和显示）
装置
6
传送解
密装置
23
电子水印
插入装置
7
PC内部
解密
装置
解密装置
11
数据通道
24 PC

图 6

版权保护的AV数据	许可应用软件	鉴定
禁止拷贝	A	成功
禁止拷贝	B	失败
禁止拷贝	C	成功
允许拷贝一次	A	成功
允许拷贝一次	B	失败
允许拷贝一次	C	成功
不允许拷贝	A	成功
不允许拷贝	B	失败
不允许拷贝	C	成功

图 7